1. Activation netGuards system

As described above, NetGuard system is activated upon receiving alerts of an attack. The system than focused on defending only the victim(s) of the attack. In the first version of the NetGuard system we assume that the information about the existing of the attack, and the information who is the victim is injected to the system from outside.

Activation the NetGuard system enforces two important change in the flow of traffic to the victim:

1. Traffic to the victim, from outside the network, and inside the network, is redirected to NetGuards.
2. Only flow that passes throw NetGuard can reach the actual victim.

In this section we describe in details one of the possible architecture and mechanism that achieve the above goals.

We give to each server IP two IP addresses. One is the server ***public address*** and the other is the ***server private address***. The *server public address* is the address of the server that is spread in the world, throw the DNS mechanism. The *server private address* is the address that known only to trustable parts of the networks, i.e., the NetGuards and to the interfaces of routers that connected to routers or netGuards (See figure 1). In other words, the *server private address* is not known to router interfaces that are connected to hosts. This give us the ability, to discard packets originated from hosts, that uses the *server private address* .

At the time of the attack all traffic to the server, which is the victim of the attack, is navigated to the NetGuard. This is done by routing any traffic using the *victim public address* to NetGuards. Hence achieving our first goal, that traffic to the victim, from outside the network, and inside the network, is redirected to NetGuards. We give below details of one of the possible ways to i redirect the traffic (see subsection 1.1)

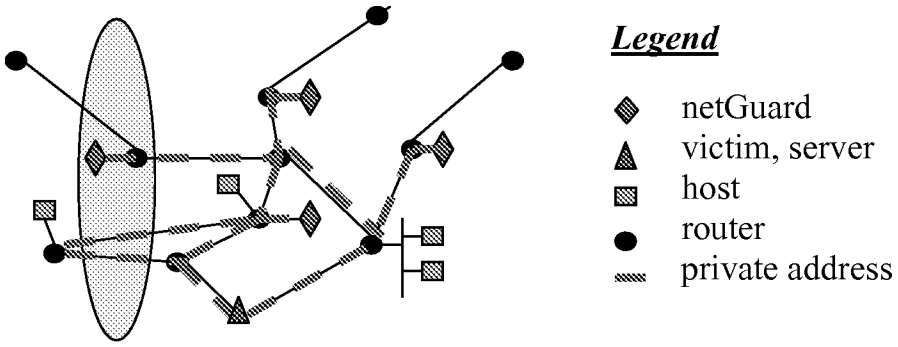


Figure 1: The *victim private address* is known only to trustable parts in the networks, i.e., the interfaces of routers that connected to another router or to netGuards. The routes in the network where the *victim private address* is known is marked by dashed red lines.

The NetGuards machine, discriminates between traffic to the victim that is part of the attack, and genuine traffic. The traffic of the attack would be blocked at NetGuards. Genuine traffic would be routed from the NetGuards to the victim, using the *victim*

private address. This would done by a simple manipulation on the destination field in the packets of the genuine traffic. Hence we achieve our second goal, and only flow that passes throw NetGuard can reach the actual victim. This is due, to the fact that in our architecture only traffic originated from NetGuard can use the *victim private address*, and hence reach the victim.

When the attack is ended, we just cancel the redirection to NetGuards, of all the traffic to the victim. Hence, again any traffic addressed *victim public address* can be routed directly to the server, which was the victim of the attack. In the following subsection we give the details of the redirection mechanism.

1.1 Redirecting traffic to NetGuards

Recall, that in case of attack we want to route any traffic addressed to the *victim public address* to NetGuards. This can be done by two different methods, one more suitable for the traffic that originated inside the network and the other more suitable to the traffic that originated outside the network.

Traffic that originated outside the network, would surly need to pass through one of the border routers, i.e., a router that surrounded the network. In our architecture a NetGuard machine is attached to each such border router. In time of attack, the control of the NetGuards system injected an update to the border router, by updating the policy routing mechanism in the router. This update, would notified the border router that any packets that is addressed to the *victim public address* would be forward to the NetGuards. Updating the policy routing mechanism, give us the ability to change the routing behavior without degrading the border routing performance[1].

In case the traffic, is originated from inside the network, one could use the same mechanism, in order to redirect the traffic addressed to the victim to the NetGuard. However, this required updating the policy routing of all the routers in the network. Hence in many cases, it more beneficial to use a different method, that is based on a simple routing manipulation. The designated NetGuard[2] that handles the inside traffic to the victim would announced its IP address as the *victim public address*, while the

---

[1] Page: 2
[0] Unlike access list, that required filtering every packet, and hence degrading the router performance, Policy routing doesnot harm the routing performance.
To understand this, we briefly explain the look up process in today routers. Most of the routers use Cisco Express Forwarding, or some equivalence mechanism. Using FEC, every interface has a cache where it store the information about the next hop for the last packets that arrive throw this interface. When packets arrive to the interface card and the destination is not store in the cache, a new forwarding process is done. This process is done in the central unit that does the lookup process for all the interfaces. This process take into account the routing policy that can be defined per interface. This operation is done rarely and in almost all of cases, the lookup operation use the cache information. Hence the impact of the degrading in the forwarding time is minor.

[2] In some case in order to handle the volume of the intra network traffic, it may beneficial to use not one NetGuards, but a farm of NetGuard However, one should noticed that the problem of attacks, and special spoofing attack, in most of the cases is harder when the attack is originated from outside the network. When the attack is originated from inside network, there is full information and management of the network. Hence ingress and egress filtering can be used, for dealing with spoofing attack. In cases when the origins of the attack are known, one can more easily stop the attack, by disable the origins of the attack.

victim server, would redraw from this address. This routing updating information, would spread quickly in the networks, using the standard routing protocol, e.g., OSPF, EIGRP or RIP.

TCP Anti-spoofing

We describe here a new anti-spoofing techniques which is TCP oriented. This anti-spoofing mechanism authenticated the genuine of the source address of the flow, based on the SYN mechanism of TCP. When a host wants to open a TCP connection with the server, the hosts sends a SYN request, notified about its wish for a new connection. The server authenticated its source address by sending him back a random number. Than, the server wait to received this number back the source. Naturally a spoofed source cannot repeat the number, and hence any connection between the server and a spoof source, is dismissed. Hence the SYN phase, which is the connection establishment phase in TCP (also called the three-way handshake), is a naturally anti-spoofing method (see figure 2).

However, since this mechanism is done by the server, the SYN mechanism has become one of the efficient way to do denial of service attack. SYN-attack, is based on the fact that the server get high volume of SYN request. This lead to the fact that the buffer, of SYN requests is filled, dismissing any new SYN requests, which can be a SYN request of a genuine host. This kind of attack also make a huge burden on the CPU server.

In our architecture we built a purposed computer, the NetGuard computers, that take the role of the server and do the SYN process. The NetGuards, can deal with a high volume of traffic, which in many cases equal to the bandwidth of the links. The architecture of the NetGuards system also distributed the load of the attack in the SYN-attack, on the number entrance points to the network.

Using a special computer for the SYN process, is very naturally solution. Also in day to day life, the job of guarding and gatekeepering is separated from the actual activity that is guarded due to performance issue.

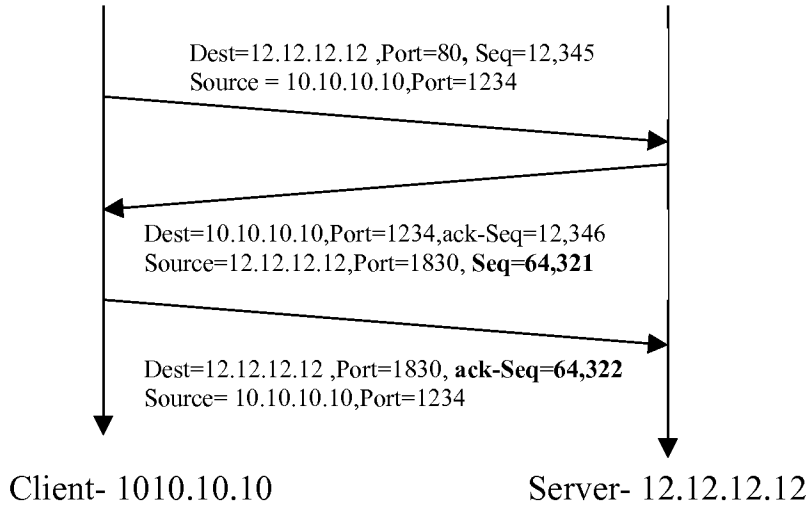
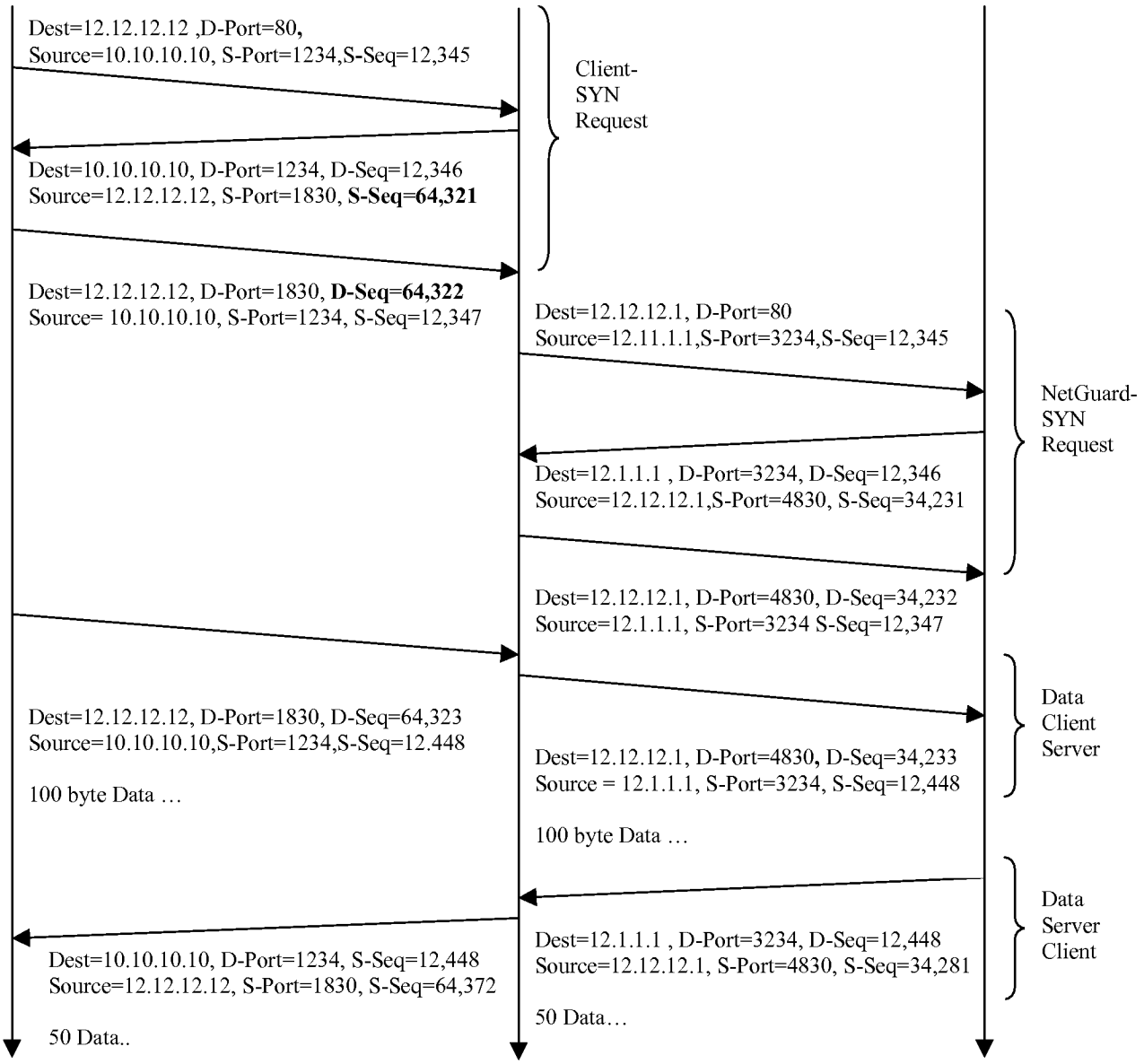


Fig 2: The SYN request.

EXHIBIT A



Client- 10.10.10.10

NetGuard – 12.1.1.1
Play the rule of 12.12.12.12
12.12.12.12 is the server public address

Server- 12.12.12.1
this address is the private address of the victim

, filling the buffer of the server, with spoofed

many spoofed source start the operation of the SYN-attack

If the source addressed is gennot spoof, than The basic idea is to send back to the source a random number.

Authenticated the source of the flow. Thus distinguish between spoof source address to real source address. The Authentication mechanism is a new anti-spoofing techniques TCP oriented

Ability to throw up -

To divide the work of the routers…